Superfund Enterprise Management System (SEMS) Application Support

(Attachment 1)

Statement of Work

1. Superfund Enterprise Management System (SEMS) Application Support

U.S. Environmental Protection Agency

Office of Land and Emergency Management (OLEM)

Office of Superfund Remediation and Technology Innovation (OSRTI)

Superfund Enterprise Management System (SEMS) Application Support

2. Background

The Environmental Protection Agency administers Superfund, the federal government's program to clean up the nation's uncontrolled hazardous waste sites. Under the Comprehensive Environmental Response Compensation and Liability Act of 1980 (CERCLA), commonly known as “Superfund,” and its amendments in 1986 and 1992 the law provided broad Federal authority to respond directly to releases or threatened releases of hazardous substances that may endanger public health or the environment.

In 2014, the Superfund Program implemented a new information system, the Superfund Enterprise Management System (SEMS). This effort included combining multiple regional records systems, the re-creation of dozens of reports and reporting data objects, replacing the legacy Comprehensive Environmental Response, Compensation and Liability Information System (CERCLIS) program data management system as well as the implementation of additional functionality supporting program management. This system currently supports data and record management and publication efforts related to cleanup activities for Sites whose characteristics fall under the umbrella of the Office of Land and Emergency Management (OLEM).

The purpose of this task is to maintain the existing system, look for opportunities to reduce operation costs and improve existing capabilities with a focus on data access, data integration, and usability. The primary business functions supported by SEMS existing capabilities are:

- High-Level site information including planning and project management including future planned obligations
- Superfund performance measure tracking in support of the Government Performance and Results Act (GPRA)
- Superfund records management and information
- Business reporting and analytics

The business functions implemented using custom designed application modules developed and implemented using Oracle tools and Technology. The modules include:

1. Database (SEMS-DB)
2. Data Warehouse (SEMS-DW)
3. Site Management Module (SEMS-SM)
4. Reports Module (SEMS-Reports)

5. Superfund Content Entry Form (SEMS-CEF)
6. Superfund Site Profile Pages (SEMS-SPP)
7. Superfund Public User Database (SEMS-SPUD)
8. SEMS-Publishing (SEMS-Pub)
9. Records Management (SEMS-RM)

3. Objectives

The goals and objectives for this task order are:

- Operate and Maintain the Superfund Enterprise Management System (SEMS)
- Improve the existing Capabilities of SEMS especially in the areas of web services, data integration, records management and usability
- Evaluate how to reduce the O&M Operating costs
- Maintain a Help Desk for user support and technical assistance
- Develop materials and provide training to support implementation of SEMS Modules which support the business functions needed to perform the Superfund mission
- Special Project SEMS Enhancements

4. Scope

The scope of work falls under Task Area IT 5 Operations and Maintenance, Task Area 6 Integration Services, and Task Area 8 Digital Government. The types of services requested shall include:

- Software Maintenance and Upgrades
- Operational Support
- Help Desk / IT Support
- IT Training
- Data Quality Management
- Requirements Analysis, Design, Coding and Testing
- Application Prototyping
- Business Intelligence and Analytics
- Database Development and Management
- IT Infrastructure Optimization
- Cloud Computing

5. Specific Tasks

5.1 Task 1 – Operation and Maintenance

The contractor shall provide support services from qualified and experienced personnel to support the planning, analysis, design, engineering, development, programming and maintenance of web and system software applications and databases.

SEMS in its current state is mature system that will not require major code development. The contractor shall provide project management, software maintenance, technical support and minor upgrades for the ongoing operations of SEMS

Specific tasks include, but are not limited to:

- Developing and releasing system enhancements to improve usability, correct minor defects, or address specific problems arising from nonstandard task orders as approved and prioritized by the SEMS Change Control Board. This should follow SDLC Best practices and include internal and regression testing and appropriate artifacts.
- Maintenance of existing reports and reporting data objects
- Documenting all defects in a government-specified defect tracking system

- Support of the Oracle OBIEE Tool including account administration and application updates and upgrades
- Maintenance and Update of existing databases
- Diagnosis of data problems through the examination of on-screen data and reports
- Coordinating with other EPA personnel at the National Computing Center (NCC)) for deployment of SEMS software
- Coordinating with other EPA personnel at NCC for testing and deployment patches and upgrades to COTS software on servers hosting SEMS
- Conduct Project Management Coordination and Planning using project management best practices. This may include, but is not limited to, schedule creation, earned value management, communication support and risk management
- Provide Capital Planning and Investment (CPIC) support including, but not limited to:
    - Updating the government – specified system (eCPIC)
    - Preparing draft and final documents for monthly OMB submissions, OEI dashboards as well as annual updates
    - Assisting SEMS team with actions related to the EPA FITARA review
    - Any other CPIC documents that may be required by OMB or the Agency
- Assist in preparing security plans, policies, guidelines, and standards for systems and system users in order to implement EPA security directives and policies.
- Review, Creation, Maintenance and Update of SEMS artifacts to ensure they accurately reflect the current implementation of SEMS. Documents include but are not limited to:
    - Data dictionaries for the SEMS “base” database, SEMS data warehouse and SPUD including legal values
    - Specifications and queries used for canned reports
    - Documentation / update of business rules relating to sites “getting credit” for actions
    - SDLC documents
    - Entity Relationship database (ER) Diagrams
    - Business and Technical Process Flows

5.2 Task 2 – Improve Existing Capabilities

The contractor shall provide support services from qualified and experienced personnel to support the planning, analysis, design, engineering, development, programming and maintenance of web and system software applications and database projects. This includes, but is not limited to:

- Organization and participation in requirements and / or user stories sessions
- Upon approval to proceed by the Government, design the necessary modifications to the system and update relevant documentation. System design shall conform to the security protocols stipulated for EPA applications.
- Perform coding, unit testing, and integration of the modified code. Participate in the test-readiness preparation activities that follow.
- Perform configuration management, including configuration identification, change control, status accounting and verification.

5.2.1 Data Web Services and APIs

- Perform necessary analysis to complete a plan of action to support the creation of web services and / or APIs that support both internal EPA and external public-access to data, records and geographic information stored in SEMS. Public release of information shall follow appropriate EPA guidelines.
- Analysis and plan of action for consuming web services and / or APIs from other EPA sources including financial, removal, enforcement, sampling and geospatial data and metadata

5.2.2 Data Architecture and Integration

- Perform necessary analysis to complete a plan of action for implementing time series reporting data objects so that values can be compared across specific time periods
- Perform necessary analysis to complete a plan of action for ingesting and / or integrating other EPA data with SEMS data including financial, removal, enforcement, sampling and geospatial data
- Perform necessary analysis to complete a plan of action to access and / or store shapefiles and other Superfund geographic boundaries created in the Regional Offices.
- Conduct necessary analysis to complete a plan of action to add additional modules to the Agency Drupal solution, (WebCMS), to support accessing database and records information similar to the existing functionality used by the Superfund Site Profile Pages.
- Perform necessary analysis to complete a plan of action for creating new and / or updating existing reporting data objects to support dynamic ad hoc analysis.

5.2.3 Improve User Experience

- Perform analysis of existing processes which update the SEMS database (via the SEMS application, batch updates, backend changes, etc…) and complete an action plan for phased implementation of enhanced auditing, performance improvements and solutions to view change history.
- Perform analysis of data transformation (ETL) from the SEMS database into the SEMS Data warehouse to validate accuracy and improve logic.
- Perform analysis and complete a Plan of action for Implementation of automated processes to validate and flag data quality and data transformation issues.
- Perform analysis of the existing SEMS Records Management (SEMS-RM) data and module and complete a plan of action to improve usability and performance. Key pain points include record indexing, search functionality, user roles and current methodology for storing records
- Perform quality review of the data migrated for the legacy CERCLIS database into the SEMS database to ensure that data points collected prior to 2011 were migrated correctly. Create plan of action for implementation to include a mix of Government and Contractor resources.
- Perform analysis of the overall SEMS GUI (all modules) and complete a plan of action to modify the screens to make them more usable with a focus on simple and intuitive design.

5.2.4 Records Management

- Perform analysis of what is needed to make SEMS a DoD 5015 compliant records management system and create a plan of action for implementation
- Perform analysis of what is needed to integrate the agency e-mail solution (Microsoft Outlook) and SEMS for capture, metadata creation and storage of email messages and attachments and records and create a plan of action for implementation for manual and batch options.

5.2.5 Business Intelligence and Analytics

- Provide analysis of existing data structures and canned reports and dashboards and create a plan of action to modify and / or create new reporting capabilities to support analysis at the lowest level of data and integration with other data sources
- Update and Modify Business Intelligence tools to support dynamic reporting, dashboards and ad – hoc analysis based on customer IT functional reporting requirements and /or user stories
- Update existing reports as necessary and creation of new capabilities and dashboards to reflect enhanced data warehouse architecture

5.3 Task 3 – Evaluate how to reduce O&M Operating Costs

The Contractor shall perform an analysis of the existing infrastructure and architecture for SEMS. The overall goal is to ensure that SEMS is “right sized” with a goal to reduce the operating costs by 50%.

SEMS is hosted at the NCC using a combination of virtual machines and dedicated servers running Linux and Windows

The implementation plan, including level of effort, should take into account the following considerations:

- The current storage for the system (including databases and files) is approximately ~30TB growing at an average rate of 2 TB per year
- An EPA – approved cloud based solution for all or portions of the system should be considered

5.4 Task 4 - Help Desk Services

The Contractor shall provide user support for the SEMS Reference Desk and the functions within SEMS. The current tools being used are JIRA for user requests and defect ticketing and JAMA for requirements and documentation support. This list may increase over time with the addition of ancillary applications. The Contractor shall provide SEMS support for the distributed network of users, such as additional EPA Regional offices, laboratories or partners. Support services shall include but are not limited to the functions in the sub – tasks sections below.

5.4.1 Staff and Maintain the SEMS Reference Desk

The Contractor shall staff and maintain the SEMS Reference Desk that responds to technical and procedural questions, and communicates the same to the system account holder network or others as designated. The Reference Desk may encompass file format and handling issues, file structure and metadata questions, standard operating procedures, content quality questions, security questions, and will route calls to subject matter experts, NCC, and others in SEMS support roles when necessary.

- The Contractor shall provide support in the creation and maintenance of system user accounts.
- The Contractor shall provide support in collecting and processing items received via telephone or e-mail and storing them in the tracking tool
- Support communication to the user community administrators and system owners about defects, enhancement issues, questions about SEMS, system components, testing and usage, System Outages, System Maintenance, Newsletter Distribution, Meeting minutes.
- Facilitate UAT by responding to questions, test results and system status reporting by regional and national EPA testers during a release testing period of any system under modification.
- The Contractor shall create and maintain documentation such as user guides and on-line help and incorporate any modifications to system functionality in existing documentation.
- The Contractor shall create and keep updated contact lists, problem reports and resolutions, exception reports, and historical documentation in a location specified by the EPA. All artifacts will require screening for duplication, relevance.

5.4.2 Ticket / Ticketing System Support

The timeframe and metrics for each of the tasks below shall be outlined in the Technical Directive. The current ticketing system is JIRA.

- The Contractor shall evaluate each item entered into the ticketing system and verify/change the type of request: defect, enhancement, issue or question.
- The Contractor shall evaluate the impacts of requests (defects and enhancements) on the application and the database.
- The Contractor shall keep the ticketing system updated and current as new user tickets arrive.
- The Contractor shall be responsible for continually processing (e.g., completing the LOE/Impact Analysis and determination as to defect or enhancement) requests.
- The Contractor shall evaluate items entered into the ticketing system after a release to determine if new defects are found in the release.

- The Contractor shall evaluate all new items entered into the ticketing system to determine if any of the new items are a question.
- In the event a question is entered into the ticketing system, the Contractor shall respond to the requestor.
- The Contractor shall respond to regional questions and test results reporting by regional and national EPA testers during the release testing period. This period includes the period of regional test as well as during the deployment of a new release and patch releases.

5.5 Task 5 – Training Support

A major factor in the success of the SEMS project is Training. SEMS typically has between 4 – 6 major releases a year and requires training to go along with these releases. To support this the Contractor will be asked to maintain and update existing training materials, create new training materials and conduct training sessions. Additional materials to facilitate communication and user outreach will be requested as well. Additionally, the Contractor shall provide support in converting training to webinar sessions when applicable.

5.5.1 Training Materials

- Provide analysis of existing training materials and a plan of action to modify them to support multiple types of users (data entry as well as data consumers and program management users).
- Provide analysis of SEMS security training and plan of action to update and enhance it on an annual basis to be updated and available before the start of the first quarter of the next fiscal year.
- Training materials may include written documentation, slide presentations, visualizations and / or webinars
- The Contractor shall modify existing and create new materials upon EPA approval

5.5.2 Provide Training

- The Contractor shall support training sessions to train OSRTI System owners and staff to train the end users. This may include meeting with requesting staff prior to trainings to understand challenges/training needs to tailor/customize the training as necessary.
- The Contractor shall also conduct remote applications training via the EPA Portal, or other appropriate technology such as web conference, teleconference and / or videoconferencing.
- Training sessions shall be recorded and/ or made available electronically as appropriate

5.6 Task 6 – Special Project SEMS Enhancements

The EPA is undergoing organizational change and as a result there may be significant enhancements and / or new modules requested in SEMS to support these efforts. Software Development activities and specialized trainings will be requested as appropriate. It is anticipated that projects of these type would vary in length from 3 to 12 months and be in addition to the activities supporting the previous subtasks.

5.7 Acronyms

The following acronyms are referenced in this document:

Abbreviation	Description
CCB	Change Control Board
CERCLA	Comprehensive Environmental Response Compensation and Liability Act
CERCLIS	Environmental Response, Compensation and Liability Information System
CO	Contracting Officer
C.O.B	Close of Business

COOP	Continuity of Operations Plan
COR	Contracting Officer's Representative
CPIC	Capital Planning and Investment Control
CR	Change Request
eCPIC	Electronic Capital Planning and Investment Control
EPA	Environmental Protection Agency
ER	Entity Relationship
ETL	Extract Transform Load
FISMA	Federal Information Security Management Act
GPRA	Government Performance and Results Act
GUI	Graphical User Interface
IMB	Information Management Branch
NCC	National Computing Center
O&M	Operations and Maintenance
OLEM	Office of Land and Emergency Management
OEI	Office of Environmental Information
OEM	Office of Emergency Management
OMB	Office of Management and Budget
OOP	Object Oriented Programming
OSRE	Office of Site Remediation Enforcement
OSRTI	Office of Superfund Remediation and Technology Innovation
PWS	Performance Work Statement
QASP	Quality Assurance Surveillance Plan
RTM	Requirements Traceability Matrix
RTP	Research Triangle Park EPA Location
SDD	System Design Document
SDLC	Software Development Lifecycle
SEMS	Superfund Enterprise Management System
SEMS-CEF	SEMS Content Entry Form Module
SEMS-DB	SEMS Database Module
SEMS-DW	SEMS Data Warehouse Module
SEMS-Pub	SEMS Publishing Module
SEMS-Reports	SEMS Reports Module
SEMS-RM	SEMS Records Management Module
SEMS-SM	SEMS Site Management Module
SEMS-SPP	SEMS Superfund Site Profile Page Module
SEMS-SPUD	SEMS Superfund Public User Database Module
SRS	Software Requirements Specification
TOCOR	Task Order Contracting Officer Representative

UAT	User Acceptance testing

6. Contract Type

The contract type is a hybrid of Time and Materials and Firm Fixed Price. Firm Fixed Price tasks include 5.1, 5.3, 5.4, and 5.5.

7. Place of Performance

Work will be performed at the Contractor's site only unless work is required to be done on site at EPA. The EPA's Office of Land and Emergency Management (OLEM) will make "hotel" space available to support collaboration.

8. Period of Performance

The base period of performance is one year (12 months) from the date of contact award. There are four option periods of one year (12 months) each.

9. Deliverables/Delivery Schedule

The following table provides the list of deliverables.

SOW TASK #	DELIVERABLE TITLE	#CALENDAR DAYS AFTER TO AWARD
5.1	Task 1 – Operation and Maintenance	
5.1.1	Source code commented and loaded into approved version control	By C.O.B. Business Day before a release to any of the Stage or Production environments.
5.1.2	Test Plans, test scripts and test results created / updated and loaded into approved version control	By C.O.B. Business Day before a release to any of the Stage or Production environments.
5.1.3	SEMS Software Requirements Specification (SRS)	Date specified in approved project and / or sprint schedule
5.1.4	SEMS Requirements Traceability Matrix (RTM) (Date specified in approved project schedule)	Date specified in approved project and / or sprint schedule
5.1.5	System Design Document (SDD)	Date specified in approved project and / or sprint schedule
5.1.6	Design Review Meeting Minutes	Date specified in approved project and / or sprint schedule
5.1.7	Wireframes	Date specified in approved project and / or sprint schedule
5.1.8	Prototype	Date specified in approved project and / or sprint schedule

5.1.9	Preliminary Design Review	Date specified in approved project and / or sprint schedule
5.1.10	Critical Design Review	Date specified in approved project and / or sprint schedule
5.1.11	Complete Application Deployment Checklist preparation and meeting materials	Date specified in approved project and / or sprint schedule
5.1.12	Rapid prototype each module as initial requirements and /or user stories sets are baselined	Date specified in approved project and / or sprint schedule
5.1.13	Maintain and refine SEMS databases	Dates specified in approved project and / or sprint schedule
5.1.14	Use App Scan, or other Agency standard code scan software. Report (Dates specified in approved project schedule, but will be a standard practice with each software delivery to the EPA NCC for loading into Staging and Production environments.)	All code updates
5.1.15	Release Notes	By C.O.B. Business Day before a release to any of the Stage or Production environments.
5.1.16	Coordinate the ADC process for implementing the SEMS changes	Biweekly and Monthly calls
5.1.17	Project Management Plan	30 business days from date of Task Order Award
5.1.18	Project Schedule	30 business days from date of Task Order Award
5.1.19	Project Schedule Updates	Every Wednesday with weekly status report
5.1.20	Project Management Plan	Draft - 15, Final - 30
5.1.21	Monthly Status Report (Technical and Financial)	Monthly, on 10th calendar day
5.1.22	Weekly Status report	Every Wednesday
5.1.23	Maintenance of SEMS Security Plan	Update with each major system code and / or database update
5.1.24	Updated Security Plan	Date specified in approved project schedule
5.1.25	Maintain relevant section(s) of the Risk Management Plan	Quarterly review

5.1.26	System Contingency Plan (Date specified in approved project schedule)	Update in synch with Security Plan
5.1.27	Test Contingency Plan	Annual test of Contingency Plan. (Date specified in approved project schedule)
5.1.28	XACTA Record – Maintain currency and accuracy of the XACTA record for SEMS.	Monthly and Annual updates
5.1.29	Monthly XACTA updates	Date specified in approved project schedule
5.1.30	Annual FISMA survey	Date specified in approved project and / or sprint schedule
5.1.31	Risk Management Plan	Date specified in approved project and / or sprint schedule
5.1.32	COOP Contingency Plan	Date specified in approved project and / or sprint schedule
5.2	Task 2 – Improve Existing Capabilities	
5.2.0.1	All Approved activities which include Software Development and Project Management will meet the deliverable requirements for Task 1	Date specified in approved project and / or sprint schedule
5.2.1	Subtask 2.1 Data Web Services and APIs	
5.2.1.1	Plan of Action for creation of web services / APIs	Date specified in approved project and / or sprint schedule
5.2.1.2	Plan of action for consuming web services / APIs	Date specified in approved project and / or sprint schedule
5.2.2	Subtask 2.2 Data Architecture and Integration	
5.2.2.1	Plan of Action for time series	Date specified in approved project and / or sprint schedule
5.2.2.2	Plan of Action for ingestion and integration	Date specified in approved project and / or sprint schedule
5.2.2.3	Plan of Action for geospatial	Date specified in approved project and / or sprint schedule
5.2.2.4	Plan of Action for Drupal	Date specified in approved project and / or sprint schedule
5.2.2.5	Plan of Action for Reporting Data Objects	Date specified in approved project and / or sprint schedule
5.2.3	Subtask 2.3 Improve User Experience	

5.2.3.1	Plan of Action for existing processes	Date specified in approved project and / or sprint schedule
5.2.3.2	Plan of Action for data transformation	Date specified in approved project and / or sprint schedule
5.2.3.3	Plan of Action for automated validation processes	Date specified in approved project and / or sprint schedule
5.2.3.4	Plan of Action for Records Management module	Date specified in approved project and / or sprint schedule
5.2.3.5	Plan of Action for CERCLIS data review	Date specified in approved project and / or sprint schedule
5.2.3.6	Plan of Action for SEMS GUI data review	Date specified in approved project and / or sprint schedule
5.2.4	Subtask 2.4 Records Management	
5.2.4.1	Plan of Action for DoD 5015 Compliance	Date specified in approved project and / or sprint schedule
5.2.4.2	Plan of Action for implementation of manual and batch options for records interface between SEMS and Outlook	Date specified in approved project and / or sprint schedule
5.2.5	Subtask 2.5 Business Intelligence and Analytics	
5.2.5.1	Plan of Action for analysis at lowest level	Date specified in approved project and / or sprint schedule
5.2.5.2	Plan of Action for BI tools modification	Date specified in approved project and / or sprint schedule
5.2.5.3	Plan of Action for updating existing reports	Date specified in approved project and / or sprint schedule
5.3	Task 3 – Reduce O&M Operating Costs	
5.3.1	Implementation plan for reducing O&M Operating costs	Date specified in approved project and / or sprint schedule
5.4	Task 4 – Help Desk Services	
5.4.1	Subtask 4.1 Staff and Maintain the SEMS Reference Desk	
5.4.1.1	Provide monthly metrics on reference desk support	Monthly, on 10th calendar day
5.4.1.2	Update on-line and user documentation based on software releases	Draft 5 days before release to STAGE, Final C.O.B 1 Business Day before release to PRODUCTION or as requested for early training
5.4.2	Subtask 4.2 Ticket / Ticketing System Support	

5.4.2.1	Update ticketing system within defined timeframe	Date specified in approved Technical Directive
5.4.2.2	Communicate with users according to the communication plan in the Technical Directive	Date specified in approved Technical Directive
5.5	Task 5 – Training Support	
5.5.1	Subtask 5.1 Training Materials	
5.5.1.1	Plan of Action on existing materials	Date specified in approved project and / or sprint schedule
5.5.1.2	Plan of Action for Security Training	Date specified in approved project and / or sprint schedule
5.5.1.3	Creation of new materials	Date specified in approved project and / or sprint schedule
5.5.2	Subtask 5.2 Provide Training	
5.5.2.1	Training plan	30 business days from date of Task Order Award
5.6	Subtask 5.6 Special Project SEMS Enhancements	
5.6.1	Plan of action for implementation of Special Project	Date specified in approved project and / or sprint schedule

10. Security

The Superfund program follows all policies and procedures set forth by the Agency. SEMS is hosted at EPA's NCC and avails itself of all aspects of NCC security controls and procedures. The NCC along with the Superfund program, have a shared security responsibility

- SEMS underwent a Privacy Impact Assessment on 10/4/2017
- System of Record Notice (SORN) completed in May 2015
- ATO - SEMS Security Plan 8/25/2017
- Last Risk Assessment – Year 1 – 11/25/2017

The NCC supports and protects the central infrastructure that runs all of the services offered at the NCC. This infrastructure is comprised of the hardware, software, networking, and the facility. For these services, NCC handles basic security tasks like managing the operating system (OS) and database patching, firewall configuration, and disaster recovery. Superfund manages the logical access controls for the resources and account credentials.

Additional services provided by the NCC are as follows:

- Physical and Environmental Security - Physical access is strictly controlled both at the perimeter and at building entrances by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. Access to the building and data center and information to employees and contractors who have a legitimate business need for such privileges. Additional controls are in place for Fire

Detection and Suppression, Power, Climate and Temperature, and monitors electrical, mechanical, and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment, along with Storage Device Decommissioning.

- Network Security – the NCC has implemented a secured network infrastructure that is carefully monitored and managed. Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services. Secure Access Points are in place to monitor inbound and outbound communications and network traffic. Transmission Protection HTTP or HTTPS using Secure Sockets Layer (SSL), a cryptographic protocol are in place to protect against eavesdropping, tampering, and message forgery.
- Fault-Tolerant Design – The NCC infrastructure has a high level of availability and has designed its systems to tolerate system or hardware failures with minimal customer impact. The NCC has in place Network Monitoring and Protection that are designed to detect unusual or unauthorized activities. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts.
- The NCC monitors the network by also reviewing information in the audit and security logs. All vulnerabilities are reported to the program and are followed up by the NCC security team.
- Application Deployment Support – Before new versions of the application is deployed, the NCC meets regularly with the program office representative to discuss requirements, any applicable security, technical, and administrative issues, passed the appropriate reviews, and verified by the customer. Once all items have passed the Application Deployment Checklist (ADC), the deployment is pushed into production.

The SEMS team is responsible for adhering to all security policies and procedures set forth by the Agency and NIST. The SEMS team is responsible for maintaining the following:

- Authorization to Operate (ATO),
- Security Plan,
- Contingency Plan,
- Mitigate all vulnerabilities form the Annual Risk Assessment,
- Perform Annual Table Top Test/Exercise,
- Account Management
- As part of maintaining the application/database code, we also track/manage audit data, and
- Ensure confidential business information (CBI) is protected through Access Controls (Account Management, Separation of Duties, Least Privilege, Unsuccessful Login Attempts, System Use Notification, Session Lock, and Supervision and Review -Account Management), Acknowledging the Rules of Behavior, and through Security Awareness and Training.

Users are assigned roles and privileges by the system administrator in Headquarters and in the regions who manage and control access to the various applications, modules, and forms in SEMS. The System Administrator role will determine which users have access to the SEMS applications, and within an application, which forms, functions, and reports a user can access. Before a user is granted access, they must complete a new user form and signed by their supervisor. Staff are then assigned particular roles, and through these roles assignments, they acquire rights “permissions” to perform particular functions. The key controls to assure that information is handled in accordance with its prescribed use include:

Technical Class Controls

- Access Controls
    - Account Management
    - Access Enforcement
    - Separation of Duties
    - Least Privilege

    - Unsuccessful Login Attempts
    - System Use Notification
    - Session Lock
    - Supervision and Review -Account Management

- Audit Controls
    - Auditable Events
    - Audit Analysis, Monitoring, and Reporting
    - Identification and Authentication

Management Class Controls

- Security Planning, Policy, and Procedures
    - Rules of Behavior
- Systems and Services Acquisition Policy and Procedures
    - Software Usage Restrictions
    - Security Engineering Principles

Operational Class Controls

- Security Awareness and Training Policy and Procedures
    - Security Awareness
    - Security Training

Implementation of these controls is documented in the SEMS System Security Plan that addresses all of the areas identified above, including how Superfund employees are granted system access based upon their organizational role and need to know, authorizing officials, technical aspects of authentication management, software use and engineering, and the auditing of access files to ensure the protection of data maintained by OSRTI.

10.1 Confidential Treatment of Sensitive Information

Information that will be captured in SEMS is derived from a variety of sources, including existing programmatic records, Agency staff and contractors, civil investigators, attorneys, and the like. As the SEMS solution will be integration of existing Superfund systems and their respective information, the information may include correspondence, reports, laboratory analyses, FOIA requests and responses, photographs, technical drawings, maps, and digital audio/video clips that are specific to the Superfund, Brownfields, Emergency Response and Prevention, Cost Recovery, Enforcement and other delegated/non-delegated EPA programs with ties to the Superfund program.

The Superfund program has taken the following steps to protect confidential information:

- All confidential documents are stored in locked file cabinets or rooms accessible only to those who have a business “need-to-know.”
- All electronic confidential information is protected via firewalls, encryption and passwords.
- Employees should clear their desks of any confidential information before going home at the end of the day.
- Employees should refrain from leaving confidential information visible on their computer monitors when they leave their work stations
- All confidential information, whether contained on written documents or electronically, should be marked as “confidential.”
- All confidential information should be disposed of properly (e.g., employees should not print out a confidential document and then throw it away without shredding it first.)

- Employees should refrain from discussing confidential information in public places.
- Employees should avoid using e-mail to transmit certain sensitive or controversial information.
- Limit/Restrict users access to the application and its data on a “need-to-know’ basis.
- Before disposing of an old computer, use software programs to wipe out the data contained on the computer or have the hard drive destroyed.
- Provide annual security training and CBI/PII training to the users of the application.
- Enforce Confidentiality Policy
- Access to the system is extremely limited to EPA staff and contractors working on Superfund related work. No one is provided access to the application without a need-to-know and approval of supervisor via user form.
- Accounts are assigned from EPA Headquarters who have personal knowledge of each individual’s need to access the information in the system.
- There is a privacy/warning notice that is displayed on each login.
- Each user must log in with a user name and password each time they access the system.

10.2 System Configuration Security

The Superfund program has developed a configuration management plan which document roles and responsibilities, resources, and formal processes and procedures to ensure that all proposed changes to the application are evaluated and approved before implementation. Activities such as system-wide upgrades, replacements, and deployments, while maintaining the appropriate level of information security. The Superfund program works with the National Computing Center (NCC) in Raleigh, NC to control, track and maintain a system configuration baseline, system changes, and licensing information. Also, existing system documentation (i.e., system security plan, system configuration documents, system maintenance records, vendor manuals, system configuration diagrams, and security-related information) are also maintained to ensure information is protected and secured.

Monthly meetings with the contracting team and NCC personnel occur to review hardware and software configurations, system architecture, and version controls. Upgrades must be approved via email or with change control forms.

11. Government Furnished Equipment (GFE)/ Government Furnished Information (GFI)

A PIV and/or PUC card are required to access the EPA environment. No other GFE is required.

12. Packaging, Packing, and Shipping Instructions

Not Applicable

13. Inspection and Acceptance Criteria

Inspection and acceptance criteria for all deliverables shall adhere to the methods standards outlined in the Quality Assurance Surveillance Plan (QASP). The contractor shall deliver a draft QASP within 15 days of contract award, with a finalized QASP (to be negotiated with the Government) delivered no later than 45 days after contract award. Example metrics are provided in Appendix B.

14. Accounting and Appropriation Data

Funds are available and will be made available for this Task Order. The Task order will be incrementally funded.

15. Other Pertinent Information or Special Considerations

1. Contractors should have experience with the following IT Development Skills:

    - Developing web – based applications using fourth generation languages such as Java is required
    - Knowledge of object – oriented programming (OOP) is required
    - Experience in database scripting, performance tuning, Extract Transform Load (ETL) is required
    - Experience in the implementation and or / use of web services and APIs is required
    - Experience in the creation of complex reporting data objects (including time series and change history) is required

2. Development will be incremental following an Agile, Incremental Waterfall or similar methodology.
3. Contractors will adhere to the EPA defined tasks related to IPN #17-01: Use of 22 Cybersecurity Tasks (See Appendix B).

4. The following EPA policies must be followed. These policies can be found at: https://www.epa.gov/irmpoli8/current-information-directives
    - CIO 2104.0 Software Management and Piracy Policy
    - CIO 2120.0 Capital Planning and Investment Control (CPIC) for the Management of Information Technology Investments
    - CIO 2121.1 System Life Cycle Management (SLCM) Policy
    - CIO 2122.1 Enterprise Architecture Policy
    - CIO 2123.1 Configuration Management Policy
    - CIO 2130.1 Section 508: Accessible Electronic and Information Technology
    - CIO 2131 National Geospatial Data Policy
    - CIO 2133.0 Data Standards
    - CIO 2134.0 Information Collection Policy
    - CIO 2135.0 Enterprise Information Management Policy (EIMP)
    - CIO 2150.1 Interim Agency Network Security Policy
    - CIO 2150.3 Environmental Protection Agency Information Security Policy
    - CIO 2150.4 Mobile Computing Policy
    - CIO 2151.1 Privacy Policy
    - CIO 2155.1 Records Management Policy
    - CIO 2157.1 Freedom of Information Act (FOIA) Policy
    - CIO 2171.0 Information Access Policy
    - CIO 2180.1 Web Governance and Management
    - CIO 2181.0 Posting Copyrighted Works on EPA Web Site

5. The SEMS project in its current state is primarily developed using an enterprise project and program management (EPPM) suite of Oracle applications. These include Oracle 11g , Business Process Management Suite with Universal Content Manager (UCM), Business Intelligence reporting and data mining tool, and custom coded components using the Oracle ADF version of Java coding language.

6. Other tools that are used include Informatica Powercenter 10.0 for ETL, Cold Fusion 9 for some web development and Kofax for scanning services

16. Post-Award Administration

Past Performance Evaluations will be completed annually and at the end of the task order.

17. Key Personnel

1. A Project Manager, a Senior Developer and a Senior Computer Systems Analyst shall be identified by name and title/job classification in offeror proposals as key personnel.

2. The Contractor agrees that the above key personnel shall not be removed from the contract effort, replaced or added to the contract without a compelling reason and without compliance with paragraphs (3) and (4) hereof. The Government will not approve substitutions for the sole convenience of the contractor.

3. If any change to the key personnel position becomes necessary (substitutions or additions), the Contractor shall immediately notify the Contracting Officer in writing, accompanied by the resume of the proposed replacement personnel who shall be of at least substantially equal ability and qualifications as the individuals currently approved for that category.

4. **No substitution or replacement** of the key personnel shall be approved **within the first ninety (90) days** after contract award.

5. All requests for approval of changes hereunder must be in writing, via email, and provide a detailed explanation of circumstances necessitating the proposed change. Request for changes should be made whenever the need is identified. Beside the resume, the request must also provide:

a. A comparison of skills and qualifications to those set forth in the accepted resume proposed for substitution;
b. A signed employee procurement integrity agreement;
c. Number of hours the contractor will provide at his/her own expense to train the proposed replacement, and
d. Any other information requested by the Contracting Officer to reach a decision.

18. Transition Plan

The Contractor shall provide for orderly close-out of the task order at the end of the period of performance. The Contractor shall develop a *Task Order Transition Plan* outlining the steps for an orderly transition to a new contract vehicle. The plan shall address at minimum creation of a task order documentation inventory, security activities related to transition, project training, and schedule for completion of activities in each area.

The Contractor shall perform at minimum activities in the following areas:

- *Task Order Documentation Inventory*. The Contractor shall conduct a physical inventory of the project and team libraries for systems documents, life cycle documents, and other documentation (e.g., third party software). Upon creation of the inventory, the Contractor shall reconcile inventoried documentation with that listed in the PWS (if applicable), review the status of all products, arrange for the return of needed documentation and disposal of all unwanted documentation, and confirm the format in which documentation shall be delivered to the EPA.
- Source Code. The Contractor shall conduct an inventory of the source code version and database structures and data against the EPA Development, Staging and Production environments and ensure that the latest versions of the code and data structures and data are the latest and / or correct version for each environment.
- Security. The Contractor shall perform the necessary activities to ensure a secure transition to a new contract/Contractor. These activities include, but are not limited to:

- Provide a list of all EPA computer accounts along with names of Contractor employees with account access under the task order.
- Provide the names of all Contractor employees with access to EPA's systems.
- Document any additional security procedures needed for, or involved in applications, databases, etc., such as library accesses or tables.
- Ensure that any EPA badges held by Contractor staff are returned to EPA.
- Discuss security issues with EPA COR / TOCOR
- Determine if debriefings on Privacy Act information or other sensitive information are appropriate for the task order.
- Project Training. A major factor in the successful transition of the task order to EPA and/or the designated Contractor is training. To facilitate training, the Contractor shall develop a *Training Plan* identifying specific training sessions, objectives, curriculum, and the appropriate documentation to be provided. Upon request from EPA, the Contractor shall conduct the transition training sessions.
- Transition Schedule. The Contractor shall monitor Transition activities and schedules to ensure completion within the transition period. The Contractor shall identify any potential conflicts that impact successful transition and notify the TOCOR when conflicts are identified.

APPENDIX A: IPN#17-01: Use of 22 Cybersecurity Tasks

Cybersecurity and Protecting Sensitive Information

Task A -	**Personally Identifiable Information Contract Closeout**
Task B -	**Contractor Return of all EPA-Provided and EPA-Activity-Related Information**
Task C -	**Verified Secure Destruction of All EPA-Provided and EPA-Activity-Related Information**
Task D -	**Contractor Return of all EPA-Owned and Leased Computing and Information Storage Equipment**
Task E -	**Authority to Operate (ATO) Suspension or Revocation**
Task F -	**Security Monitoring and Alerting Requirements**
Task G -	**IT Security and Privacy Awareness Training**
Task H -	**Specialized Information Security Training for Staff with Significant Security Responsibilities**
Task I -	**Federal Reporting Requirements**
Task J -	**Protecting Sensitive Information**
Task K -	**Security Assessment and Authorization (SA&A)**
Task L -	**Contractor System Oversight/Compliance**
Task M-	**Contractor Access to EPA IT Systems**
Task N -	**Individual Notification for Personally Identifiable Information**
Task O -	**Credit Monitoring and Identity Protection**
Task P -	**Compliance with IT Security Policies**
Task Q-	**Secure Technical Implementation**
Task R -	**Internet Protocol Version 6 (IPv6)**
Task S -	**Cloud Service Computing**
Task T-	**Contract Performance Information and Testimony**
Task U -	**Rehabilitation Act Section 508 Standards**
Task V -	**Termination for Default - Failure to Report Information Security Incident**

Task A - Personally Identifiable Information Contract Closeout

a) *Definition.* Personally Identifiable Information (PII) - as defined in OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, PII refers to sensitive information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

b) *Certification of Sanitization of EPA-provided and EPA-Activity-Related Files and Information (including but not limited to all records, files, and metadata in electronic or hardcopy format).* As part of contract closeout, the Contractor shall submit a *Certification of Sanitization of EPA-provided and EPA-Activity-Related Files and Information* to the Contracting Officer and the Contracting Officer's Representative (COR) following the template provided in Appendix G of National Institute of Standards and Technology (NIST) Special Publication 800-88, *Guidelines for Media Sanitization Revision 1*, which assesses risk associated with Personally Identifiable Information (PII) that was generated, maintained, transmitted, stored or processed by the Contractor. The Senior Agency Official for Privacy (SAOP) shall review the Certification and coordinate with the Contracting Officer and the COR.

c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task B - Contractor Return of all EPA-Provided and EPA-Activity-Related Information

a) Within thirty (30) days (or a different time period approved by EPA) of an EPA request, or after the end of the contract performance period, the Contractor must return all originals of all EPA-provided and EPA-Activity-Related Information (including but not limited to all records, files, and metadata in electronic or hardcopy format). The Contractor must return originals obtained while conducting activities in accordance with the contract with EPA; or distributed for any purpose by the Contractor to any other related organization and/or any other component or separate business entity; or received from the Contractor by any other related organization and/or any other component or separate business entity. Contractors must return all originals so that they cannot be used for further business by Contractor.

b) Concurrent with the return of all originals as set forth in paragraph (a), the Contractor must document to the EPA the return of all originals of all EPA-provided and EPA-Activity-Related Information (including but not limited to all records, files, and metadata in electronic or hardcopy format). The Contractor must document originals obtained while conducting activities in accordance with the contract with EPA; or distributed for any purpose by the Contractor to any other related organization and/or any other component or separate business entity; or received from the Contractor by any other related organization and/or any other component or separate business entity.

c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task C - Verified Secure Destruction of All EPA-Provided and EPA-Activity-Related Information

a) Within 60 days after the end of the contract performance period or a time period approved by EPA, or after the contract is suspended or terminated by EPA for any reason, and after EPA has accepted and approved the Contractor's return of information, the Contractor must execute secure destruction (either by the Contractor or third-party firm approved in advance by EPA) of all existing active and archived originals and/or copies of all EPA-provided and EPA-activity-related

files and information (including but not limited to all records, files, and metadata in electronic or hardcopy format). This information includes but is not limited to information obtained by the Contractor while conducting activities in accordance with the contract with EPA; or distributed for any purpose by the Contractor to any other related organization and/or any other component or separate business entity; or received from the Contractor by any other related organization and/or any other component or separate business entity. Destruction Methods shall be by procedures approved by EPA in advance in writing.

b) Within 75 days after the end of the contract performance period or a time period approved by EPA, or after the contract is suspended or terminated by EPA for any reason, and after EPA has accepted and approved the Contractor's return of information, the Contractor must document to the EPA the secure destruction of all existing active and archived originals and/or copies of all EPA-provided and EPA-activity-related files and information, (including but not limited to all records, files, and metadata in electronic or hardcopy format). This information includes but is not limited to information obtained by the Contractor while conducting activities in accordance with the contract with EPA; or distributed for any purpose by the Contractor to any other related organization and/or any other component or separate business entity; or received from the Contractor by any other related organization and/or any other component or separate business entity. Destruction Methods shall be by procedures approved by EPA in advance in writing.

c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task D - Contractor Return of all EPA-Owned and Leased Computing and Information Storage Equipment

a) Within 60 days (or a different time period approved by EPA) after the end of the contract performance period, the Contractor must return all EPA-owned and leased computing and information storage equipment to EPA.

b) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task E - Authority to Operate (ATO) Suspension or Revocation

a) *Definitions*.

   a. *Authority to Operate (ATO)* - Signed by the Agency chief information officer (CIO) or deputy CIO, ATOs are issued for all information systems that input, store, process, and/or output Government information. In order to be granted an ATO, all federal information systems must be compliant with National Institute of Standard and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, and FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. Contractors whose internal information systems will process Sensitive Information incidental to Agency product or service development must meet requirements for NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, instead of NIST SP 800-53.

   b. *ii) Information Security Incident* - an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. The Contractor must report all known Information Security Incidents if they involve Sensitive Information.

c. *Sensitive Information* - As defined in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Sensitive Information is any information where the loss, misuse or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. Sensitive Information is subject to stricter handling requirements than non-sensitive information because of the increased risk if the data are compromised. Some categories of Sensitive Information include Financial, Medical or Health, Legal, Strategic and Business, Human Resources, Personally Identifiable Information (PII), and Sensitive PII. These categories of information require appropriate protection as stand-alone information and may require additional protection in aggregate.

b) In the event of an Information Security Incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this requirement, the Contracting Officer may direct the Contractor to take additional security measures to secure Sensitive Information. These measures may include restricting access to Sensitive Information on the Contractor information technology (IT) system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the Sensitive Information from the Internet or other networks or applying additional security controls.

c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task F - Security Monitoring and Alerting Requirements

a) All Contractor-operated systems that use or store EPA information must meet or exceed EPA policy requirements pertaining to security monitoring and alerting. All systems are subject to the requirements of existing federal law, policy, regulation and guidance (e.g., Federal Information Security Management Act of 2002). The Contractor must comply with the EPA-used Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) policy for security monitoring and alerting, which includes requirements not limited to:
    a. System and Network Visibility and Policy Enforcement at the following levels:
        i. Edge
        ii. Server / Host
        iii. Workstation / Laptop / Client
        iv. Network
        v. Application
        vi. Database
        vii. Storage
        viii. User

b) Alerting and Monitoring

c) System, User, and Data Segmentation

d) (b) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task G - IT Security and Privacy Awareness Training

a) The Contractor must ensure that all Contractor personnel complete EPA-provided mandatory

security and privacy training prior to gaining access to EPA information systems. Non-compliance may result in denial of system access.

b) The Contractor must ensure that all Contractor personnel complete security and privacy refresher training on an annual basis. EPA will provide notification and instructions to the Contractor on completing this training.

c) The Contractor must ensure that each Contractor employee review and sign the *EPA Rules of Behavior* pertaining to appropriate use of EPA information systems prior to gaining access to EPA information systems. The Contractor must also ensure that each Contractor employee reviews these *EPA Rules of Behavior* at least annually. EPA will provide notification to the Contractor when these reviews are required.

d) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task H - Specialized Information Security Training for Staff with Significant Security Responsibilities

a) The Contractor must ensure that Contractor personnel with significant information security responsibilities complete specialized information security training based on the requirements defined in the EPA role-based training program *(program provided after Contract award)*. The objective of the information security role-based training is to develop an EPA information security workforce with a common understanding of the concepts, principles, and applications of information security to ensure the confidentiality, integrity and availability of EPA's information and information systems. The Contractor is required to report training completed to ensure competencies are addressed. The Contractor must ensure employee training hours are satisfied in accordance with EPA Security and Privacy Training Standards *(provided after Contract award)*. The Contracting Officer's Representative (COR) will provide additional information for specialized information security training based on the requirements in paragraph (b).

b) The following role-based requirements are provided:

    a. not applicable

c) The Contractor must ensure that all IT and Information Security personnel receive the necessary technical (for example, operating system, network, security management, and system administration) and security training to carry out their duties and maintain certifications.

d) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task I - Federal Reporting Requirements

a) Contractors operating information systems on behalf of EPA must comply with Federal Information Security Modernization Act (FISMA) 44 USC Section 3541 reporting requirements. Annual and quarterly data collection will be coordinated by EPA. Contractors must provide EPA with the requested information based on the timeframes provided with each request. Contractor systems must comply with monthly data feed requirements as coordinated by EPA. Reporting requirements are determined by the Office of Management and Budget (OMB), and may change for each reporting period. The Contractor will provide the EPA Contracting Officer's Representative (COR) with all information to fully satisfy FISMA reporting requirements for Contractor systems.

b) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task J - Protecting Sensitive Information

a) Definitions.

a. Sensitive Information.

(1) As defined in National Institute of Standards and Technology Special Publication (NIST SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Sensitive Information is any information where the loss, misuse or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. Sensitive Information is subject to stricter handling requirements than non-sensitive information because of the increased risk if the data are compromised. Some categories of Sensitive Information include Financial, Medical or Health, Legal, Strategic and Business, Human Resources, Personally Identifiable Information (PII), and Sensitive PII. These categories of information require appropriate protection as stand-alone information and may require additional protection in aggregate.

b. Personally Identifiable Information (PII).

(1) PII, as defined in OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, refers to sensitive information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment made by the EPA Privacy Officer of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information that is publicly available — in any medium and from any source — is or can be combined to identify an individual. As an example, PII includes a name and an address because it uniquely identifies an individual, but alone may not constitute Sensitive PII.

c. Sensitive PII.

(1) Sensitive PII refers to personally identifiable information that can be used to target, harm, or coerce an individual or entity, assume or alter an individual's or entity's identity, or alter the outcome of an individual's or entity's activities. Sensitive PII requires stricter handling than PII because of the increased risk to an individual or associates if the information is compromised. Some categories of Sensitive PII include stand-alone information, such as Social Security numbers (SSN) or biometric identifiers. Other information such as a financial account, date of birth, maiden names, citizenship status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also considered Sensitive PII. In addition, the context of the information may determine whether it is sensitive, such as a list of employees with poor performance ratings or a list of employees who have filed a grievance or complaint.

b) Authorization to Use, Store, or Share Sensitive Information.

a. Through the Contracting Officer, the Contractor must obtain written approval by the Chief Information Officer (CIO) or designee prior to the use or storage of EPA Sensitive Information, or sharing of EPA Sensitive Information by the Contractor with any subcontractor, person, or entity other than the EPA.
b. The Contractor shall not remove Sensitive Information from approved location(s), electronic device(s), or other storage systems, without prior approval of the CIO or designee obtained through the Contracting Officer.

c) *Information Types*. Sensitive Information includes PII, which in turn includes Sensitive PII. Therefore, all requirements for Sensitive Information apply to PII and Sensitive PII, and all requirements for PII apply to Sensitive PII.

d) *Information Security Incidents.*

a. An *Information Security Incident* is an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. The Contractor must report all known Information Security Incidents if they involve Sensitive Information.
b. Information Security Reporting Requirements.
(1) The Contractor must report all Information Security Incidents and Privacy Breaches in accordance with the requirements below, even if it is believed the Incident may be limited, small, or insignificant. An information security report shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for Sensitive Information, or has otherwise failed to meet contract requirements.
(2) The Contractor must report via email all Information Security Incidents and Privacy Breaches to the EPA Service Helpdesk immediately, but not later than 30 minutes, after becoming aware of the Incident. The Contractor shall email the EPA Service Helpdesk at CSIRC@epa.gov, and shall also email the Contracting Officer and Contracting Officer Representative (COR). If the Contractor fails to report in 30 minutes, specific Government remedies may include termination in accordance with EPA Requirement *Termination for Default – Failure to Report Information Security Incident*.
(3) The types of information required in an Information Security Incident and Privacy Breach reports include: Contractor name and point-of-contact (POC) information, Contract number; the type, amount and description of information compromised; and incident details such as location, date, method of compromise, and impact, if known.
(4) The Contractor shall not include any Sensitive Information in the subject or body of any e-mail. To transmit Sensitive Information, the Contractor shall use Federal Information Processing Standards (FIPS) 140-2 compliant encryption modules to protect Sensitive Information in attachments to email.
(5) If applicable, the Contractor must also provide supplemental information or reports related to a previously reported incident directly to the Contracting Officer, COR and EPA Service Helpdesk at CSIRC@epa.gov. The Contractor shall include any related ticket numbers in the subject line of the email.
c. Information Security Incident Response Requirements.
(1) All determinations related to Information Security Incidents and Privacy

Breaches, including response activities, notifications to affected individuals and related services (e.g., credit monitoring and identity protection) will be made in writing by authorized EPA officials at EPA's discretion and communicated by the Contracting Officer.

(2) The Contractor must provide full access and cooperation for all activities determined by EPA to be required to ensure an effective Incident Response, including providing all requested images, log files, and event information to facilitate rapid resolution of Information Security Incidents. The Contractor shall maintain the capabilities to: determine what sensitive information was or could have been accessed and by whom, construct a timeline of user activity, determine methods or techniques used to access the information, identify the initial attack vector, and remediate and restore the protection of information. The Contractor is required to preserve all data, records, logs and other evidence that are reasonably necessary to conduct a thorough investigation of the Information Security Incident.

(3) The Contractor is responsible for performing Incident and Privacy Breach Response activities required by EPA, including but not limited to inspections, investigations, forensic reviews, data analyses and processing by EPA and EPA OIG personnel and others on behalf of EPA. As requested by the Contracting Officer, the Contractor may provide technical support for the Government's final determinations of responsibility activities for the Incident and/or liability activities for any additional Incident Response activities (e.g., possible restitution calculation to affected individuals).

(4) EPA, at its sole discretion, may obtain the assistance of Federal agencies and/or third-party firms to aid in Incident Response activities.

(5) The Contractor is responsible for all costs and related resource allocations required for all subsequent Incident Response activities determined to be required by EPA.

e) Contractor Plan for Protection of Sensitive Information.

a. The Contractor is responsible for the proper handling and protection of Sensitive Information to prevent unauthorized disclosure. Upon contract award, the Contractor shall develop and maintain a documentation plan addressing the following minimum requirements regarding the protection and handling of Sensitive Information:
b. Proper marking, control, storage and handling of Sensitive Information residing on electronic media, including computers and removable media, and on paper documents.
c. Proper control and storage of mobile technology, portable data storage devices, and communication devices.
d. Proper use of Federal Information Processing Standards (FIPS) 140-2 compliant encryption modules to protect Sensitive Information while at rest and in transit throughout EPA, Contractor, and/or subcontractor networks, and on host and client platforms.
e. Proper use of FIPS 140-2 compliant encryption modules to protect Sensitive Information in email attachments, including policy that passwords must not be communicated in the same email as the attachment.
~~f.~~ *Information Security Incidents*. The Contractor shall report to the Government any security incident involving Personally Identifiable Information (PII) of which it becomes aware.
g. Contractor Access to EPA IT Systems. The Contractor shall configure their network to support access to government systems (e.g., configure ports and protocols for access).

h. Requirement for Business to Government (B2G) network connectivity. The Contractor will connect to the B2G gateway via a Contractor-procured Internet Service Provider (ISP) connection, and assume all responsibilities for establishing and maintaining their connectivity to the B2G gateway. This will include acquiring and maintaining the circuit to the B2G gateway, and acquiring a FIPS-140-2 Virtual Private Network (VPN)/Firewall device compatible with the Agency's VPN device. Maintenance and repair of contractor procured VPN equipment shall be the responsibility of the Contractor.

i. Dial-Up ISP Connections are not acceptable.

j. The Contractor must comply with the Agency's Guidance regarding allowable ports, protocols and risk mitigation strategies (e.g. File Transfer Protocol or Telnet).

k. IT Security and Privacy Awareness Training. The Contractor must ensure annual security education, training, and awareness programs are conducted for their employees performing under the subject contract that addresses, at a minimum, physical security, acceptable use policies, malicious content and logic, and non-standard threats such as social engineering for their employees. The Contractor must also ensure employees performing under the subject contract receive the Agency's initial and annual information security awareness training.

l. The Contractor must not conduct default installations of "out of the box" configurations of Commercially Off the Shelf (COTS) purchased products. The contractor shall configure COTS products in accordance with EPA, NIST, Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) or Center for Internet Security (CIS) standards. Standards are listed in order of precedence for use. If standards do not exist from one of these sources, the contractor shall coordinate with EPA to develop a configuration.

f) *Subcontract flowdown*. The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task K - Security Assessment and Authorization (SA&A)

a) The Contractor is required to undergo Security Assessment and Authorization (SA&A); i.e., the process by which a federal agency examines its information technology infrastructure and develops supporting evidence necessary for security assurance accreditation, prior to using information systems to access and/or store Government information, potentially including Sensitive Information. The Contractor's facilities must also meet the security requirements for "moderate confidentiality impact" as defined by the Federal Information Processing Standards (FIPS) 199 publication *Standards for Security Categorization of Federal Information and Information Systems*.

b) For all information systems that will input, store, process, and/or output Government information, the contractor shall obtain an Authorization to Operate (ATO) signed by the Chief Information Officer (CIO) from the Contracting Officer (working with the Contracting Officer's Representative (COR)) before using EPA information in the system. The contractor may be able to obtain an Authorization to Test from the SIO for the office obtaining services that will allow use of EPA information in certain circumstances to facilitate system development or implementation. Before a federal information system can be granted an ATO, it must be compliant with National Institute of Standard and Technology (NIST) SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, and FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. Contractors whose internal information systems will process Sensitive Information incidental to Agency product or service development must meet requirements for NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* (instead of NIST SP 800-53) in order to be granted an ATO.

c) FIPS 199 moderate confidentiality impact must be utilized for Contractor information technology (IT) systems and security control baseline requirements.
d) Prior to Agency SA&A activities, the COR must complete a Privacy Threshold Analysis (PTA) for all IT systems. Then the COR must provide the completed PTA to the EPA Privacy Officer for a determination of whether a Privacy Impact Assessment (PIA) is required. If a determination is made that a PIA is required, it will be completed by EPA in accordance with EPA PIA Template instructions.
e) The Contractor is responsible for preparing SA&A documentation with the use of EPA tools and security documentation templates including System Security Plan, Security Assessment Report, Contingency Plan, and Incident Response Plan. The Contractor must follow federally mandated SA&A and Risk Management Framework (RMF) processes throughout the IT system lifecycle process to ensure proper oversight by EPA. RMF modifies the traditional Certification and Accreditation process and integrates information security and risk management activities into the system development life cycle.
f) The Contractor must submit SA&A documentation as defined in paragraph (e) to the COR at least 60 days before the ATO expiration date.
g) The Contractor shall fix or mitigate system or security vulnerabilities within a time frame commensurate with the level of risk (as identified by the EPA and Contractor) they present:
    a. High Risk = 2 business days from vulnerability notification from contractor
    b. Moderate Risk = 7 business days from vulnerability notification from contractor
    c. Low Risk = 30 business days from vulnerability notification from contractor
h) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task L - Contractor System Oversight/Compliance

a) Pursuant to National Institute of Standards and Technology Special Publication (NIST SP) 800-53 Rev 4, the EPA and GAO have the authority to conduct site reviews for compliance validation and will conduct security reviews on a periodic and event-driven basis for the life of the contract. Full cooperation by the Contractor is required for audits and forensics.
b) The Contractor shall provide EPA access to the Contractor's facilities, installations, operations, documentation, databases, information technology (IT) systems and devices, and personnel used in performance of the contract, regardless of the location. The Contractor shall provide access to the extent required, in EPA's judgment, to conduct an inspection, evaluation, investigation or audit, including vulnerability testing to safeguard against threats and hazards to the integrity, availability and confidentiality of agency data or to the function of information technology systems operated on behalf of agency, and to preserve evidence of information security incidents. This information shall be available to the EPA upon request.
c) All Contractor systems used in the performance of the contract must comply with Information Security Continuous Monitoring (ISCM) and Reporting as identified in OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*. In addition, EPA reserves the right to perform ISCM and IT security scanning of Contractor systems with tools and infrastructure of EPA's choosing.
d) All Contractor systems used in the performance of the contract must perform monthly vulnerability scanning as defined by EPA IT and Security Policy, and the Contractor must provide scanning reports to the Contracting Officer, who will forward them to the EPA CIO or designee on a monthly basis.
e) All Contractor systems used in the performance of the contract must participate in the implementation of automated security controls testing mechanisms and provide automated test results in Security Compliant Automation Protocol (SCAP) compliant data to the Contracting

Officer, who will forward to the EPA CIO or designee on a monthly basis.

f) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task M - Contractor Access to EPA IT Systems

a) Immediately following contract award, the Contractor shall provide to the Contracting Officer's Representative (COR) a complete list of Contractor employee names that require access to EPA information systems.

b) The Contractor shall provide a Contractor employee change report by the fifth day of each month after contract award to the COR. The report shall contain the listing of all Contractor employees who separated or were hired under the contract in the past 60 days. This report shall be submitted even if no separations or hires have occurred during this period. Failure to submit a Contractor employee change report may, at the Government's discretion, result in the suspension of all network accounts associated with this contract. The format for this report will be provided by the COR.

c) The Contractor shall require each of its employees who will need system access for six months or less to utilize a Personal Identity Verification-Interoperable (PIV-I) card or equivalent, as determined by EPA, in order to access EPA information technology (IT) systems and Sensitive Information. The Contractor shall ensure that its employees will not share accounts to access EPA IT systems and Sensitive Information.

d) The Contractor shall require each of its employees who will need system access for more than six months to utilize an HSPD-12 compliant Personal Identity Verification (PIV) card, such as the EPA EPASS card, in order to access EPA IT systems and Sensitive Information. The Contractor shall ensure that its employees complete a federal government-initiated background investigation as part of the PIV issuance process. The Contractor shall ensure that its employees will not share accounts to access EPA IT systems and Sensitive Information.

e) EPA, at its discretion, may suspend or terminate Contractor access to any systems, information/data, and/or facilities when an Information Security Incident or other electronic access violation, use or misuse issue warrants such action. The suspension or termination shall last until EPA determines that the situation has been corrected or no longer exists. Upon request by EPA, the Contractor shall immediately return all EPA information/data, as well as any media type that houses or stores Government information.

f) The Contractor shall notify the COR at least five days prior to a Contractor employee being removed from a contract (notification shall be at least 15 days for key personnel in accordance with requirement 1552.237-72, *Key Personnel*). For unplanned terminations or removals of Contractor employees from the Contractor organization that occur with less than five days notice, the Contractor shall notify the COR immediately. The Contractor shall ensure that HSPD-12/PIV cards issued to a Contractor's employee shall be returned to the COR prior to the employee's departure.

g) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task N - Individual Notification for Personally Identifiable Information

a) Definitions.

   a. *Information Security Incident* is an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

b. *Personally Identifiable Information (PII)*, as defined in OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, refers to sensitive information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment made by the EPA Privacy Officer of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information that is publicly available — in any medium and from any source — is or can be combined to identify an individual. As an example, PII includes a name and an address because it uniquely identifies an individual, but alone may not constitute Sensitive PII.

c. *Sensitive PII* refers to personally identifiable information that can be used to target, harm, or coerce an individual or entity, assume or alter an individual's or entity's identity, or alter the outcome of an individual's or entity's activities. Sensitive PII requires stricter handling than PII because of the increased risk to an individual or associates if the information is compromised. Some categories of Sensitive PII include stand-alone information, such as Social Security numbers (SSN) or biometric identifiers. Other information such as a financial account, date of birth, maiden names, citizenship status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also considered Sensitive PII. In addition, the context of the information may determine whether it is sensitive, such as a list of employees with poor performance ratings or a list of employees who have filed a grievance or complaint.

b) The Contractor shall have in place procedures and the capability to notify any individual whose Personally Identifiable Information (PII) resided in the Contractor information technology (IT) system at the time of an Information Security Incident not later than five business days after being directed by the Contracting Officer to notify individuals, unless otherwise approved by the Contracting Officer. The procedures must be approved by the EPA prior to use. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval, by the Contracting Officer in consultation with authorized EPA officials at EPA's discretion. The Contractor shall not proceed with notification unless the Contracting Officer has determined in writing that notification is appropriate.

c) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:
   a. A brief description of the incident;
   b. A description of the types of PII and Sensitive PII involved;
   c. A statement as to whether the PII or Sensitive PII was encrypted or protected by other means;
   d. Steps individuals may take to protect themselves;
   e. What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
   f. Information identifying who individuals may contact for additional information, including Contractor name and point of contact (POC) and contract number.

d) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task O - Credit Monitoring and Identity Protection

a) Definitions.

a. *Information Security Incident* is an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
b. *Personally Identifiable Information (PII)*, as defined in OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, refers to sensitive information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment made by the EPA Privacy Officer of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information that is publicly available — in any medium and from any source — is or can be combined to identify an individual. As an example, PII includes a name and an address because it uniquely identifies an individual, but alone may not constitute Sensitive PII.
c. *Sensitive PII* refers to personally identifiable information that can be used to target, harm, or coerce an individual or entity, assume or alter an individual's or entity's identity, or alter the outcome of an individual's or entity's activities. Sensitive PII requires stricter handling than PII because of the increased risk to an individual or associates if the information is compromised. Some categories of Sensitive PII include stand-alone information, such as Social Security numbers (SSN) or biometric identifiers. Other information such as a financial account, date of birth, maiden names, citizenship status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also considered Sensitive PII. In addition, the context of the information may determine whether it is sensitive, such as a list of employees with poor performance ratings or a list of employees who have filed a grievance or complaint.

b) *Credit Monitoring Requirements*. In the event that an Information Security Incident involves PII or Sensitive PII, the Contractor may be required to do the following tasks as directed by the Contracting Officer:
a. Provide notification to affected individuals as described in the "Individual Notification for Personally Identifiable Information" requirement;
b. Provide credit monitoring and identity protection services to individuals whose data was under the control of the Contractor or resided in the Contractor information technology (IT) system at the time of the Information Security Incident for a period beginning the date of the Incident and extending not less than 18 months from the date the individual is notified; and/or
c. Use a dedicated call center; or establish one if necessary and as authorized in writing by the Contracting Officer. Call center services provided by the Contractor shall include:
i. A dedicated telephone number for affected individuals to contact customer service within a fixed time period as determined by the Contracting Officer;
ii. Information necessary for affected individuals to access credit reports and credit scores;
iii. Weekly reports submitted to the Contracting Officer's Representative (COR) on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or EPA, as appropriate), and other key metrics;
iv. Escalation of calls that cannot be handled by call center staff to call center management or EPA for resolution, as appropriate;
v. Preparation of customized frequently-asked-questions-and-answers (FAQs), in consultation as applicable with other parties like subject matter experts and CORs, and that must be approved in advance in writing by the Contracting Officer; and

vi. Information for affected individuals to contact customer service representatives and fraud resolution representatives for credit monitoring and identity protection assistance.

c) *Credit monitoring and identity protection services.* At a minimum, the Contractor shall provide the following credit monitoring and identity protection services:
   a. Triple credit bureau monitoring with Equifax, Experian and Transunion;
   b. Daily customer service;
   c. Alerts provided to the individual for changes in credit posture and fraud; and/or
   d. Assistance to the individual with enrollment in the services and the use of fraud alerts.

d) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task P - Compliance with IT Security Policies

a) Information systems and system services provided to EPA by the Contractor must comply with current EPA information technology (IT), IT security, physical and personnel security and privacy policies and guidance, and EPA Acquisition Regulation 1552.211-79, *Compliance with EPA Policies for Information Resources Management*.

b) Contractors are also required to comply with current Federal regulations and guidance found in the Federal Information Security Modernization Act (FISMA) of 2014, Privacy Act of 1974, E-Government Act of 2002, Federal Information Processing Standards (FIPS), the 500- and SP500- and 800-Series Special Publications (SP), Office of Management and Budget (OMB) memoranda and other relevant Federal laws and regulations that are applicable to EPA.

c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task Q - Secure Technical Implementation

a) The Contractor shall use applications that are fully functional and operate correctly as intended on systems using the United States Government Configuration Baseline (USGCB).

b) The Contractor's standard installation, operation, maintenance, updates, and/or patching of software must not alter the configuration settings from the approved USGCB configuration.

c) Contractor applications designed for normal/regular, i.e., non-privileged end users must run in the standard user context without elevated system administration privileges.

d) The Contractor shall apply due diligence at all times to ensure that Federal Information Processing Standard (FIPS) 199 "moderate confidentiality impact" security is always in place to protect EPA systems and information.

e) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task R - Internet Protocol Version 6 (IPv6)

a) In accordance with EPA technical standards, all system hardware, software, firmware, and/or networked component or service (voice, video, or data) utilized, developed, procured, acquired or delivered in support and/or performance of this contract shall be capable of transmitting, receiving, processing, forwarding, and/or storing digital information across system boundaries utilizing system packets that are formatted in accordance with commercial standards of Internet Protocol version 6 (IPv6) as set forth in the USGv6 Profile (NIST Special Publication 500-267)

and corresponding declarations of conformance defined in the USGv6 Test Program. In addition, devices and systems shall maintain interoperability with IPv4 products.

b) Any IP product or system utilized, developed, acquired, produced or delivered must interoperate with both IPv6 and IPv4 systems and products, in an equivalent or better way than current IPv4 capabilities with regard to functionality, performance, management and security; and have available contractor/vendor IPv6 technical support for development and implementation and fielded product management.
c) As IPv6 evolves, the Contractor shall upgrade or provide an appropriate migration path for each item developed, delivered or utilized, at no additional cost to the Government. The Contractor shall retrofit all non-IPv6 capable equipment, as defined above, which is fielded under this contract with IPv6 capable equipment, at no additional cost to the Government.
d) The Contractor shall provide technical support for both IPv4 and IPv6.
e) All Contractor-provided system or software must be able to operate on networks supporting IPv4, IPv6, or one supporting both.
f) Any product whose non-compliance is discovered and made known to the Contractor within one year after acceptance shall be upgraded, modified, or replaced to bring it into compliance, at no additional cost to the Government.
g) EPA reserves the right to require the Contractor's products to be tested within an EPA or third-party test facility to demonstrate contract compliance.
h) In accordance with FAR 11.002(g), this acquisition must comply with the National Institute of Standards and Technology (NIST) US Government (USG) v6 Profile and IPv6 Test Program. The Contractor shall fund and provide resources necessary to support these testing requirements, and it will not be paid for as a direct cost under the subject contract.
i) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task S - Cloud Service Computing

a) The Contractor handling EPA information or operating information systems on behalf of EPA must protect EPA information and information systems against unauthorized access, use, disclosure, disruption, modification, or destruction per the Federal Information Security Modernization Act (FISMA) and EPA policy.
    a. EPA information stored in a cloud environment remains the property of EPA, and not the Contractor or cloud service provider (CSP). The Contractor may also be the CSP. EPA retains ownership of the information and any media type that stores Government information.
    b. In the event the Contractor is the CSP or can control the CSP through a subcontracting or other business relationship then the following requirements will apply:
b) The CSP does not have rights to use the EPA information for any purposes other than those explicitly stated in the contract or applicable "Rights in Data" contract requirements.
c) The CSP must protect EPA information from all unauthorized access.
d) The CSP must allow EPA access to EPA information including data schemas, metadata, and other associated data artifacts that are required to ensure EPA can fully and appropriately retrieve EPA information from the cloud environment that can be stored, read, and processed.
e) The CSP must have been evaluated by a Third Party Assessment Organization (3PAO) certified under the Federal Risk and Authorization Management Program (FedRAMP). The Contractor must provide the most current, and any subsequent, Security Assessment Reports to the Contracting Officer's Representative (COR) for consideration by the Information Security Officer (ISO) as part of the Contractor's overall Systems Security Plan.
f) The Contractor must require the CSP to follow cloud computing contract best practices identified in "Creating Effective Cloud Computing Contracts for the Federal Government" produced by the

Federal Chief Information Officer (CIO) Council and Federal Chief Acquisition Officers Council.

a. The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task T - Contract Performance Information and Testimony

a) Dissemination of Contract Performance Information.

a. The Contractor must not publish, permit to be published, or distribute to the public, any information, oral or written, concerning the results or conclusions made pursuant to the performance of this contract, without the prior written consent of the Contracting Officer. A copy of any material proposed to be published or distributed must be submitted to the Contracting Officer for written approval prior to publication.

b) Contractor Testimony.

a. All requests for the testimony of the Contractor or its employees, and any intention to testify as an expert witness relating to: (a) any work required by, and or performed under, this contract; or (b) any information provided by any party to assist the Contractor in the performance of this contract, must be immediately reported to the Contracting Officer.

c) *Subcontract flowdown*.

a. The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task U - Rehabilitation Act Section 508 Standards

a) All electronic and information technology (EIT) procured through this contract must meet the applicable accessibility standards at 36 CFR 1194, unless a FAR 39.204 exception to this requirement exists. 36 CFR 1194 implements Section 508 of the Rehabilitation Act of 1973, as amended, and is viewable at http://www.access-board.gov/sec508/508standards.htm.

b) The following standards are determined to be applicable to this contract:

a. 1194.21. Software applications and operating systems
b. 1194.22. Web-based intranet and Internet information and applications
c. 1194.23 Telecommunications products
d. 1194.24 Video and multimedia products
e. 1194.25 Self-contained, closed products
f. 1194.26 Desktop and portable computers
g. 1194.31 Functional performance criteria
h. 1194.41 Information, documentation, and support

c) EPA is required by Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), to offer access to electronic and information technology for disabled individuals within its employment, and for disabled members of the public seeking information and services. This access must be comparable to that which is offered to similar individuals who do not have disabilities. Standards for complying with this law and any future updates are prescribed by the Architectural and Transportation Barriers Compliance Board ("The Access Board").

d) Contractor deliverable(s) must comply with these standards.

e) The final work product must include documentation that demonstrates or provides assurance that the deliverable conforms to the Section 508 Standards promulgated by the Access Board.

f) In the event of a dispute between the Contractor and EPA, EPA's assessment of the Section 508 compliance will control and the Contractor will make any additional changes needed to conform with EPA's assessment, at no additional charge to EPA.

g) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder,

provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task V - Termination for Default - Failure to Report Information Security Incident

a) Definition. *Information Security Incident* is an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

b) If the Contractor was aware of an Information Security Incident and did not disclose it in accordance with the requirements specified in this contract or misrepresented relevant information to the Contracting Officer, the Government may terminate the contract for default, debar the Contractor from Government contracting, or pursue such other remedies as may be permitted by law or this contract.

c) *The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer*

APPENDIX B – Example Performance Metrics

Desired Outcomes	Required Services	Performance Standard	Acceptable Quality Level (AQL)	Monitoring Method	Incentives/ Disincentives